Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Факультет електроніки
Кафедра звукотехніки та реєстрації інформації

**НАУКОВО-ТЕХНИЧНА КОНФЕРЕНЦІЯ СТУДЕНТІВ**

***Сучасні проблеми застосування електронних та інформаційних технологій в телекомунікаціях, телебаченні та цифровому кінематографі***

25 травня 2017 р.

КИЇВ

## Секція С
## ЕЛЕКТРОМАГНІТНА СУМІСНІСТЬ, БЕЗПЕКА МОБІЛЬНИЙ ЗВ'ЯЗОК, СУПУТНІ ПРОБЛЕМИ ЗАСОБІВ ТЕЛЕКОМУНІКАЦІЙ

**Керівник к.т.н., доцент Пілінський В.В.**
**Секретар асистент Д.В. Тітков**

# АНАЛІЗ МОЖЛИВИХ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

***Пасько В.П.***
*КПІ ім. Сікорського кафедра звукотехніки та реєстрації інформації*

На сьогоднійшній момент інформація стає найважливішим стратегічним ресурсом. Саме тому інформація потребує особливого захисту. Поряд з терміном «захист інформації» також широко використовується термін «інформаційна безпека». Якщо захист інформації характеризує процес створення умов, що забезпечують необхідну захищеність інформації, то інформаційна безпека відображає досягнутий стан такої захищеності.

Проблема інформаційної безпеки набула особливої значущості в сучасних умовах широкого застосування автоматизованих інформаційних систем, заснованих на використанні комп'ютерних і телекомунікаційних засобах. При забезпеченні інформаційної безпеки стали цілком реальними загрози, викликані навмисними (зловмисними) діями людей. Перші повідомлення про факти несанкціонованого доступу до інформації були пов'язані, в основному, з хакерами, або «електронними розбійниками». Останнім десятиліттям порушення захисту інформації прогресує з використанням програмних засобів і через глобальну мережу Інтернет. Досить поширеною загрозою інформаційної безпеки стало також зараження комп'ютерних систем так званими вірусами.

Під загрозою безпеки комп'ютерних систем (КС) розуміються можливі дії, здатні прямо або опосередковано завдати шкоди її безпеки.

Необхідність класифікації загроз інформаційної безпеки КС обумовлена тим, що інформація, що зберігається і оброблюється в сучасних КС схильна до дії надзвичайно великого числа чинників, в силу чого стає неможливим формалізувати завдан-

ня опису всіх загроз. Тому для системи, що захищається, зазвичай визначають не повний перелік загроз, а перелік класів загроз.

Умисні загрози пов’язані з цілеспрямованими діями порушника. В якості порушника може бути службовець, відвідувач, конкурент, найманець і т. д.

Несанкціонований доступ – найбільш поширений і різноманітний вид комп'ютерних порушень. Суть НСД полягає в отриманні користувачем(порушником) доступу до об'єкту порушуючи правила розмежування доступу, встановлені відповідно до прийнятої в організації політики безпеки. НСД використовує будь-яку помилку в системі захисту і можливий при нераціональному виборі засобів захисту, їх некоректній установці і налаштуванні. НСД може бути здійснений як штатними засобами АС, так і спеціально створеними апаратними і програмними засобами.

Основні канали НСД, через які порушник може отримати доступ до компонент АС і здійснити розкрадання, модифікацію і/або руйнування інформації:

– штатні канали доступу до інформації(термінали користувачів, оператора, адміністратора системи; засоби відображення і документування інформації; канали зв'язку) при їх використанні порушниками, а також законними користувачами поза межами їх повноважень;

– технологічні пульти управління;

– лінії зв'язку між апаратними засобами АС;

– побічні електромагнітні випромінювання від апаратури, ліній зв'язку, мереж електроживлення і заземлення та ін.

В сучасних умовах безпека інформаційних ресурсів може бути забезпечена тільки комплексною системою захисту інформації. Комплексна система захисту інформації повинна бути: безперервною, плановою, цілеспрямованої, конкретної, активної, надійною. Система захисту інформації повинна спиратися на систему видів власного забезпечення, здатного реалізувати її функціонування не тільки в повсякденних умовах, але і в критичних ситуаціях.

**Перелік посилань:**

1. Семененко В.А. Информационная безопасность: Учебное пособие. 2-е изд., стереот. – М.: МГИУ, 2005. – 215 с.

2. Корнюшин, П.Н. Информационнаябезопасность / П.Н. Корнюшин, С.С. Костерин. – Владивосток: ТИДОТ ДВГУ, 2003. – 154 с.

3. Конев И. Р. Информационнаябезопасностьпредприятия / И. Р. Конев, А. В. Беляев. – СПб. : БХВ-Петербург, 2003. – 747 с.

4. Кавун С.В. Інформаційна безпека. Навчальний посібник. Ч.1/С.В. Кавун, В.В. Носов, О.В. Мажай. – Харків: Вид. ХНЕУ, 2008. – 352 с.

5. И.В. Аникин, В.И. Глова, Л.И. Нейман, А.Н. Нигматуллина Теория информационной безопасности и методология защиты информации // Учебное пособие. Казань: Изд-во Казан. гос. техн. ун-та, 2008 с. 358.

*Науковий керівник д.т.н., професор Савченко Ю.Г.*